In the Claims

The following listing of claims will replace all previous listings of claims in the Application:

1. (Presently Amended) A method of establishing an initial quantum key using ~~performing~~ quantum key distribution (QKD) with weak optical pulses, comprising:

a) at a first QKD station initially having no shared quantum key with a second QKD station:

~~a)~~ generating a random set of initial key bits k_1, k_2, ...ki...kn;

~~b)~~ encrypting the initial key bits; ~~and~~

~~c)~~ using the encrypted initial key bits to form encrypted qubits from the optical pulses without first forming unencrypted qubits from the optical pulses;

b) at the second QKD station:

receiving and measuring the encrypted qubits;

decrypting the measured encrypted qubits so as to recover a corresponding set of the key bits; and

processing the initial and recovered sets of key bits to establish the initial quantum key at the first and second QKD stations.

2. (Original) The method of claim 1, including:

encrypting the key bits using a stream cipher.

3. (Previously Amended) The method of claim 2, wherein the stream cipher uses a password formed from a fraction of a QKD key.

4. (Previously Amended) The method of claim 2, including decoding the encrypted qubits using the stream cipher.

5. (Presently Amended) A method of establishing an initial quantum key using ~~performing~~ quantum key distribution (QKD) using weak optical pulses, comprising:

at a first QKD station initially having no shared quantum key with a second QKD station:

~~a)~~ generating a random set of key bits;

~~b)~~ generating a pad using a stream cipher;

~~c)~~ XOR-ing the key bits and the pad to obtain encrypted key bits: ~~and~~

~~d)~~ modulating the weak optical pulses using the encrypted key bits so as to simultaneously encode and encrypt the optical pulses to form encrypted qubits;

at the second QKD station optically coupled to the first QKD station:

receiving and measuring the encrypted qubits using a random basis;

recovering at least a subset of the key bits from the measured encrypted qubits by XOR-ing the measured encrypted qubits with the pad; and

processing the recovered subset of key bits to establish the initial quantum key at the first and second QKD stations.

6. Canceled.

7. (Presently Amended) The method of claim ~~6~~ 5, further including:

establishing a sifted key between the first and second QKD stations based on the key bits generated in the first QKD station and the key bits recovered in the second QKD station.

8. (Presently Amended) A QKD system, comprising:

a) a first QKD station initially having no shared quantum key and having:

a. an optical radiation source adapted to emit weak optical pulses of radiation;

b. a first random number generator adapted to generate random numbers for use as first key bits;

c. a first e/d module coupled to the first random number generator to encrypt the key bits thereby forming encrypted key bits;

d. a modulator arranged to receive the weak optical pulses and adapted to modulate the polarization or phase of the weak optical pulses based on the encrypted key bits to form encrypted qubits without ~~having to~~ first ~~form~~ forming unencrypted qubits;

e. a first controller configured to control the operation of the first QKD station;

b) a second QKD station initially having no shared quantum key and optically coupled to the first QKD station and having:

a. a second modulator adapted to receive and randomly polarization-modulate or phase-modulate the encrypted qubits;

b. a detector for detecting the modulated encrypted qubits; ~~and~~

c. a second e/d module coupled to the detector and adapted to recover from the modulated encrypted qubits second key bits corresponding to the first key bits; and

d. a second controller operably coupled to the first controller, wherein the first and second controllers are configured to run QKD procedures to establish an initial quantum key between the first and second QKD stations from the first key bits and the recovered second key bits.

9-13. Canceled.